(51) International Patent Classification [6] : A63F 9/22	A1	(11) International Publication Number: **WO 98/52664** (43) International Publication Date: 26 November 1998 (26.11.98)

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: WEISS, Steven, A. [US/US]; 3300 Birtcher Drive, Las Vegas, NV 89118 (US). CARLSON, Rex, R. [US/US]; 3300 Birtcher Drive, Las Vegas, NV 89118 (US).

(74) Agent: KRETEN, Bernhard; Suite 245, 77 Cadillac Drive, Sacramento, CA 95825 (US).

(54) Title: GAMING DEVICE SECURITY SYSTEM: APPARATUS AND METHOD

(57) Abstract

A gaming device security system (10) is disclosed which includes two processing areas (20, 60) linked together and communicating critical gaming functions via a security protocol wherein each transmitted gaming function includes a specific encrypted signature to be decoded and validated before being processed by either processing area. The two processing areas (20, 60) include a first processing area (20) having a dynamic RAM and an open architecture design which is expandable without interfering or accessing critical gaming functions and a second "secure" processing area (60) having a non-alterable memory for the storage of critical gaming functions therein.

Gaming Device Security System: Apparatus and Method

Technical Field

The present invention relates generally to gaming devices, and in particular, to an advanced video and slot gaming device security system having dual processing areas with a master/slave relationship wherein the master includes a secure processing area including critical gaming functions stored and executed from a non-alterable media by the secure processing area while allowing the slave processing area to have an open architecture which is expandable without compromising critical gaming functions and retaining the ability for regulatory validation of the secure processing area of the system.

Background Art

Traditional gaming devices are based around a simple processor unit including a random number generator, an accounting means operatively coupled to a static/battery backed random access memory, and an EPROM having stored therein the important gaming functions. In addition, these gaming devices include gaming displays, coin acceptors, bill validators and hoppers operatively coupled to the simple processor. These gaming devices are relatively simple and limited in scope, usually consisting of a single executing program utilizing straight forward interrupt schemes and detection loops for asynchronous events for simple evaluation. It is also a simple matter of operatively coupling an external program validation device to the EPROM for providing effective regulatory validation of critical gaming functions to preclude unauthorized tampering or modification of the gaming machine through software. In addition, an external device validation process for suspicious jackpots or disputes may be validated by simply reading the static/battery backed random access memory associated with the simple processor. Furthermore, software developers in the gaming industry are hesitant to include compromising code in traditional gaming devices due to the ease of both internal and regulatory review.

Currently, most casinos protect their large jackpots by sealing the EPROM devices containing critical code for game functions with serialized tape, and validating the code contents against a standard after a large win.

Today's trend in gaming devices is towards an increasing utilization of personal computer based gaming platforms. Personal computer based platforms are being employed by designers to make use of real time operating systems which allow for multi-threaded/multi-tasking processes and the use of many "off the

5 shelf" device drivers. While at first, this may seem an advantage, it is not a wise choice in an environment requiring high security and regulatory monitoring. Designs of this nature elude validation by regulatory authorities in two areas, initial laboratory evaluation and field validation. Any in depth review of a PC based gaming device is both difficult and far from definitive, requiring tremendous

10 engineering resources and specialist in computer security which are expensive and normally available only on a consultant basis. Even if these resources were available, it is impossible to study the hundreds of thousands of lines of source code comprising all of the elements of such a system. In addition, the time involved in just learning how to build the executable code from the source for correlation is

15 time and resource prohibited. The multi-threaded/multi-tasking process nature of the programs in these devices make it extremely difficult to locate any compromising code which becomes clandestine since the actual sequence of the execution is hidden to the evaluating engineer. Furthermore, the code set for a complex PC device may not be fully embraced by the evaluating engineer.

20 The significant reduction of risk for detection in compromising the more complex code is an invitation to inside compromise by device designers. Further, PC based devices are simply not field verifiable, rendering any gaming jurisdiction's device inspection program or any other field validation effort useless for this gaming equipment. For example, the device must be essentially disassembled so

25 that all BIOS EPROMs and any other software located in peripheral devices may be inspected. If CD ROMs or disk drives are used, these must also be read and verified, requiring a significant amount of time. A thorough inspection program will, of necessity, be extended in scope to include hardware since the device must be searched for approved peripherals that may modify the source code execution and

30 function of the game. Hardware inspections are not easily defined, requiring a high level of technical skill for field personnel. Even if this capability is provided, each inspection will be time intensive thereby significantly reducing the effectiveness of any inspection program.

Even with these efforts, validation will not be absolute. Regardless of the extent of the inspection, it is impossible to guarantee that an approved program is actually executing from dynamic RAM. Large jackpot validations by the casino are also out of the question for the same reason. This is a result of the fact that programs executing in dynamic RAM are self modifiable and extremely difficult to extract from an operating device. The dynamic RAM only exists in an active operating context; therefore it is impossible to be sure of an accurate program validation during an evaluation to resolve questionable operation or a patron dispute.

At a time when regulatory goals should be to enhance slot machine security to protect the integrity of gaming, the introduction of these types of devices is an antithesis. These devices are an invitation to highly technical and non-detectable compromise by experts. At first, it may seem restrictive to prevent this type of design by regulation. However, multi media capabilities which can be offered via today's high technology can provide a very marketable scheme to patrons, therefore, alternative designs must be considered to provide these features in a responsible manner.

Therefore, a need exists for an independent secured processor design for validation which would provide all key functions such as the determination of game outcome, monetary input, output, and logging of relevant events. Furthermore, a need exists for an open architecture design, for example, a personal computer based design of the gaming device which would provide all shell functions of presenting the game environment and thus providing a substantial entertainment component of the gaming device. Therefore, even though compromise is still possible at the shell level, evidence of what should have occurred is recoverable from the specially designed secured processor.

Disclosure of Invention

The present invention is distinguished over the known prior art in a multiplicity of ways. For one thing, the present invention provides a video and slot gaming device security system including two processing areas linked together via a secure protocol. In addition, the present invention includes a non-alterable storage media having gaming critical functions, at a minimum, stored therein and executed from the non-alterable media by one of the two processing areas. The other

processing area of the present invention includes an open architecture design which is expandable without compromising the critical gaming functions. Thus, the present invention encourages innovations of gaming devices without reducing the effectiveness of regulatory evaluation and validation processes of the critical gaming functions. Furthermore, the present invention allows for correlating true game results and monetary transactions to player presentation under suspicious circumstances, even if the open architecture processing area is tampered with.

In one preferred form, the present invention includes at least one video and/or slot gaming device. The gaming device is based around the secure processing area which includes a random number generator, an accounting and log means operatively coupled to a static or non-volatile random access memory and an EPROM having stored therein the critical gaming functions. Preferably, a coin acceptor, a bill validator and a hopper are operatively coupled to the secured processing area. In addition, the present invention includes the open architecture processing area linked to the secure processing area and communicating therewith via the secure protocol. Furthermore, a display means is operatively coupled to a visual display for displaying, *inter alia* , random outcomes.

The open architecture design includes an internal alterable program storage media operatively coupled to a dynamic ram. Thus, the open architecture processing area allows for the storage of, *inter alia*, interactive multi media gaming functions.

In one scenario, at least one gaming device is actuated by inserting a coin in the coin acceptor or a bill in the bill validator. Gaming activity is then initiated by the player and a gaming outcome is influenced by the random number generator. The gaming outcome is then transmitted to the open architecture processing area to be animated on the visual display operatively coupled to the open architecture processing area. If the gaming outcome is a winning outcome the secure processor communicates with or drives the hopper so that a player winning on the gaming device can receive money back from a dispensing tray. Alternatively, the secure processing area may be provided with means to bestow credits as a function of the random gaming outcome.

The critical gaming functions of the present invention are stored in and executed directly from a media which is not alterable through any use of circuitry or

programming of the gaming device itself and are verifiable as to content
independent of any function of the gaming device. Critical gaming functions
include a unique control of, or any interruption of signals from a component
involved in a monetary transaction, including, coin acceptors, bill validators,
5   hoppers, interfaces to cashless wagering systems, associated equipment used in the
determination of a progressive or bonus award value or any device which provides
for the input or collection of credits, wagers or awards. In addition, critical gaming
functions also include all accounting functions including the direct and unique
control of electro-mechanical and electronically stored meters, and the result of the
10   random number generator utilized in determining game outcome. Furthermore,
critical gaming functions include a unique control over a storage and retrieval of a
historical log documenting credits, wagers, award transactions, random values used
in determining game outcome and any security or error events for the most recent
game player or games in progress and a plurality of games prior to the current or
15   most recent game. This log is to be maintained in tact for a predetermined
minimum period of time and after a power loss to the gaming device.

Furthermore, critical gaming functions may be partitioned from other
functions by executing critical gaming functions on a separate dedicated processor
and partitioning the devices hardware so that the functions not deemed critical
20   which are stored or executed from alterable media are not capable of directly
modifying the random access memory used by the critical gaming functions. Any
component required to be uniquely controlled by the critical gaming functions are
preferably not accessible by other functions stored or executed from alterable media.
Thus, the non-alterable media containing the critical gaming functions is easily
25   verifiable as to content independent of any function of the gaming device itself.

Industrial Applicability

The industrial applicability of this invention shall be demonstrated through
discussion of the following objects of the invention.

Accordingly, it is an object of the present invention to provide a new and
30   novel gaming device security system: apparatus and method.

A further object of the present invention is to provide a gaming device
security system as characterized above which includes two processing areas wherein
a second processing area is sequestered for securing critical gaming functions and a

first processing area is of an open architecture design expandable without any interference or access to the critical gaming functions stored within the second processing area.

Another further object of the present invention is to provide a system as characterized above which provides a security link operatively coupled between the first processing area and the second processing area for transmitting encrypted data correlative to critical gaming functions between the second processing area and the first processing area.

Another further object of the present invention is to provide a gaming device security system as characterized above which includes an accessible access means for coupling an external program validation device to an electronically programmable read only memory included in the second processing area.

Another further object of the present invention is to provide a gaming device security system as characterized above which includes an accessible access means for operatively coupling an external device validation process means to a static/battery backed random access memory included in the second processing area for validating suspicious jackpots and/or disputes.

Another further object of the present invention is to provide a gaming device security system as characterized above which precludes counterfeiting, tampering or modification of critical gaming functions including random outcomes and accounting logs of gaming results.

Another further object of the present invention is to provide a gaming device security system as characterized above which can be operatively coupled to an external source for downloading software into the gaming device.

Another further object of the present invention is to provide a gaming device security system as characterized above which includes a visual display for displaying decrypted random gaming outcome from the first processing area which has been transmitted thereto in an encrypted form by the second processing area via a security protocol.

Another further object of the present invention is to provide a gaming device security system as characterized above including a non-alterable memory means for storing critical gaming functions therein.

Another further object of the present invention is to provide a gaming device security system as characterized above which includes a security protocol for transmitting all critical gaming functions over a link coupling the first processing area with the second processing area.

Viewed from a first vantage point, it is an object of the present invention to provide a gaming machine comprising, in combination: a first processor having a visual display and a communication interface; a second processor sending communicating data with the first processor via the communicating interface, the second processor having means for sensing wagering activity and means for transmitting a random gaming outcome to the first processor to be animated on the visual display, the second processor provided with means to bestow credits as a function of the random gaming outcome.

Viewed from a second vantage point, it is an object of the present invention to provide a method for providing gaming security, the steps including: sequestering gaming functions into two processing areas, and linking the two processing areas via a security protocol.

Viewed from a third vantage point, it is an object of the present invention to provide a gaming device security system operatively coupled to at least one gaming machine, the system comprising in combination: a first processing means operatively coupled to and driving a visual display; a second processing means operatively coupled to the first processing means and communicating therewith via a secure protocol; a plurality of inputs enabled by a player allowing the player to initiate and sustain game play on at least the one gaming machine; the second processing means including means for determining random outcomes of game play and means for transmitting the outcomes to the first processing means for updating the visual display; a player memory card including memory storage means on the card removable from and accessible by to the second processing means to upload and download information between the second processing means and the player memory card reflective of status of an ongoing game.

Viewed from a fourth vantage point, it is an object of the present invention to provide a gaming device security system, comprising in combination: a first processor; a second processor including a non-alterable memory means for storing critical gaming functions therein; a communication link operatively coupled to the

first processor and the second processor for transmitting encrypted data packets correlative of the critical gaming functions and outcomes.

These and other objects will be made manifest when considering the following detailed specification when taken in conjunction with the appended
5   drawing figures.

Brief Description Of Drawings

Figure 1 is a schematic depiction of the present invention according to one form.

Figure 2 is a plan front view of a gaming machine.

10   Figure 3 is a flow chart of a method according to one form of the present invention of a typical game sequence of the second processing area.

Figure 4 is a flow chart of a typical poll processing logic method of the first processing area according to one form of the present invention.

Figure 5 is a flow chart of typical poll processing logic method of the second
15   processing area according to one form of the present invention.

Figure 6 is a detailed block diagram of the second processing area according to one form of the present.

Figure 7 is a detailed block diagram of a first processing area according to one form of the present.

20   Figure 8 is a drawing reflecting the interaction between a player memory card and a source of uploading and downloading.

Best Mode(s) for Carrying Out the Invention

Considering the drawings, wherein like reference numerals denote like parts throughout the various drawing figures, reference numeral 10 is directed to the
25   gaming device security system according to the present invention.

In its essence, and referring to figures 1 and 2, the gaming device security system 10 is preferably housed within a gaming device 100 which may take the form of, for example, a video and/or a mechanical reel type slot machine. The gaming device security system 10 includes a first processing area 20 and a second processing
30   area 60 operatively coupled to one another via a communication link 30. The communication link 30 provides the means for transmitting encrypted data, correlative to critical gaming functions, between the second processing area 60 and the first processing area 20. The first processing area 20 is operatively coupled to a

visual display 50 for displaying, *inter alia*, gaming graphics and random gaming outcomes. The second processing area 60 of the system 10 includes means for sensing wagering activity and means for transmitting the random gaming outcomes to the first processing area 20 such that the outcome is animated on the visual display 50. In addition, the second processing area 60 includes means to bestow credits and/or monitory awards as a function of the random gaming outcome. Furthermore, the second processing area 60 can be directly accessed for validating the outcome of any game and the outcome can be displayed on the visual display 50, on an LCD display 55 or presented visually or audibly or any other peripheral.

More specifically, and referring to figures 1 and 2, the gaming device security system 10 is operatively coupled to at least one video and/or slot gaming device 100. Figure 2 shows an example of a video slot device 100 supporting the visual display 50 and including the coin acceptor 52 , the bill validator 54, a cash out button 102, a service button 104, a bet one button 106, a display of features button 108 having scroll buttons 110, 112 disposed on either side, a spin reel button 114 and a play max button 116. In addition, the video slot device 100 includes a card reader 122, a card reader display 120 and a manual eject button 124.

The gaming device 100 is founded on the first and second processing areas 20, 60 linked together via a secure protocol. The first processing area 20 is of an open architecture design which includes an internal alterable program storage media 24 operatively coupled to a dynamic RAM means 26. Thus, the open architecture design of the first processing area 20 allows for the storage of, *inter alia*, interactive multi-media gaming functions. In addition, the first processing area 20 may be operatively coupled to an external source, for example, a remote computer 140 for downloading software into the gaming device 100 with out having access to or interfering with critical gaming functions stored in the second processing area 60. In addition, the first processing area 20 is operatively coupled to a visual display 50 for providing visual feedback to a gaming player.

The second processing area 60 is a secure processing area which includes, a watchdog circuit 61, a random number generator 62, an accounting and log means 64 operatively coupled to a static or non-volatile random access memory 66 and an electronically programmable read only memory 68 having stored therein the critical gaming functions. The second processing area 60 is operatively coupled to the

visual display 50, a coin acceptor 52, a bill validator 54, a hopper 56 and electro-mechanical meters 58 which are preferably supported by the gaming device 100. In addition, the second processing area is coupled to associated gaming equipment 120 used in the determination of a progressive or bonus award value. The second
5   processing area 60 is linked to the first processing area 20 with a communication link 30 which provides the link for transmitting data via the security protocol thereby precluding any alteration of the critical gaming functions.

The critical gaming functions are stored in and executed directly from the read only memory 68 which is not alterable through any use of circuitry or
10 programming of the gaming device 100 itself and are verifiable as to content independent of any function of the gaming device 100.

Critical gaming functions preferably include a unique control of, or any interruption of signals from a component involved in a monetary transaction, including, coin acceptors, bill validators, hoppers, interfaces to cashless wagering
15 systems, associated equipment used in the determination of a progressive or bonus award value or any device which provides for the input or collection of credits, wagers or awards. In addition, critical gaming functions also include all accounting functions including the direct and unique control of electro-mechanical and electronically stored meters, and the result of the random number generator
20 utilized in determining game outcome. Furthermore, critical gaming functions include a unique control over a storage and retrieval of a historical log documenting credits, wagers, award transactions, random values used in determining game outcome and any security or error events for the most recent game player or games in progress and a plurality of games prior to the current or
25 most recent game. This log is to be maintained in tact for a predetermined minimum period of time and after a power loss to the gaming device.

Furthermore, critical gaming functions are partitioned from other functions by executing critical gaming functions on the second processing area 60. Functions not deemed critical may be stored or executed from the alterable media 24 which is
30 not capable of directly modifying the random access memory 66 or the electronically programmable read only memory 68 used by the critical gaming functions. Any component required to be uniquely controlled by the critical gaming functions are preferably not accessible by other functions stored or executed from the alterable

media 24. Thus, the non-alterable media containing the critical gaming functions is easily verifiable as to content independent of any function of the gaming device 100 itself.

In general, the gaming device 100 is actuated by, for example, inserting a coin in the coin acceptor 52 or a bill in the bill validator 54. Gaming activity is then initiated by the player and a gaming outcome is influenced by the random number generator 62. The gaming outcome is then transmitted, via the secure protocol, to the open architecture processing area 20 and animated on the visual display 50. If the gaming outcome is a winning outcome the second processing area 60 communicates with or drives the hopper 56 so that a player winning on the gaming device 100 can receive money back from a dispensing tray 48. Alternatively, the secure processing area may be provided with means to bestow credits as a function of the random gaming outcome. The credits are preferably displayed to the player via the display 50.

More specifically, and referring to figure 3, the first processing area 20 may be referred to as a white box while the second processing area 60 may be referred to as a black box. With this terminology in mind one method of a typical game sequence with respect to the black box can be explored. Initially, a player places funds into the gaming device 100 via the coin acceptor 52 , bill validator 54 or by inserting a card into a card reader 122. The player further interacts with the gaming device 100 by placing a bet by actuating the bet one button 106, placing a max bet by actuating the play max button 116, actuating game play via, for example pushing the spin reel button 114 , or inserting further funds into the gaming device 100.

If a bet is placed, the second processing area 60 determines if the number of credits is greater than zero and if so increments the wager amount and decrements the credits which the player holds. The amount of the wager is then transmitted to the first processing area 20 or white box in an encrypted format such that the white box can update the visual display means 50. Once this transmission has been completed the second processing area or black box determines whether the wager amount is equal to a pre-determined max bet amount. If the wager amount is equal to the max bet amount the black box determines the game outcome and increments all meters associated therewith. This game outcome is then transmitted in an encrypted form via the communication link 30 to the first processing areas 20 or

between the black and white box. Once the outcome has been transmitted to the white box a query for an end of game display sequence is sent to the white box and this transmission continues until the display sequence is complete. Once the display sequence is complete the visual display is updated accordingly, the game

5   sequence loops back to a subsequent start of game.

Alternatively, if a max bet means is initially actuated, the second processing area 60 determines if the number of credits the player has is greater than or equal to the pre-determined amount of the max bet. If the player does not have enough credits to cover the max bet the black box remains at the start of the game sequence.

10   If the player has enough credits to cover the max bet the wager amount is incremented while the player's credit amount is decremented. The amount of the wager is then transmitted to the first processing area 20 or white box in an encrypted format via the communication link 30. The first processing area 20 then updates the visual display 50 accordingly. The game outcome is then determined and all

15   meters associated with the gaming device 100 are incremented if necessary. This game outcome is then transmitted in an encrypted form via the communication link 30 to the first processing area 20 or between the black and white box and the white box then updates the visual display means 50. Once the game outcome has been determined and displayed a query for an end of game display sequence is

20   looped into action and displayed on the visual display 50 until the display sequence is complete. Once the display sequence is complete the visual display is updated accordingly and the game sequence loops back to a subsequent start of game.

At the start of any game sequence the player has the option of actuating game play by, for example, pushing a spin or draw button which will result in the black

25   box determining the outcome of the game if the player has placed a wager amount which is greater than zero. If the player has not placed a wager the black box will remain in the start of the game sequence. However, if the player has placed a wager the outcome of the game is determined and then transmitted to the white box in an encrypted form via the communication link 30. Once again a query for end of game

30   display sequence is looped into action and displayed on the display 50 until the sequence is completed and then subsequently the visual display 50 is updated and a new start of game sequence is initiated.

Initially inserting funds into the gaming device 100 causes the wager amount to be incremented and transmitted to the white box in an encrypted form such that the white box will update the visual display 50. Inserting further funds into the gaming device 100 without actuating a bet, max bet or game play option will cause
5   this process to continue until the insertion of funds has equaled the max bet amount. When this occurs the game is actuated and the outcome is determined. This outcome increments all associated gaming meters and is sent to the white box in an encrypted form which in turn initiates the query for the end of game display sequence to be initiated on the visual display 50. This continues until the display
10 sequence is complete. Once the display sequence is completed the visual display is updated and the start of game sequence is initiated.

Figures 4 and 5 detail a poll processing logic method between the black box side and the white box side, the two processing areas 20, 60, of the system 10.

Referring to figure 4, when a message is be sent from the black box to the
15 white box the black box increments a message sequence number and resets a retry counter included in the second processing area 60. Next, the black box 60 builds an encrypted message and transmits this message via the communication link 30. In addition, the black box starts a message timer and a byte timer included in the second processing area 60.

20 Meanwhile, and referring to figure 5, the white box 20 tests for incoming data words. When an incoming data word is found the white box decrypts the transmitted message and builds a message packet. The white box continues to receive the incoming data word and decrypts and builds the message packet until the message packet is complete. Once the message packet is complete the white box
25 determines if the decrypted message packet is valid and if so then discerns whether the message itself is of a valid type. Once the white box has validated the message packet and determined that the message is a valid one it processes the message and constructs a response. The response is encrypted and sent back to the black box side. Alternatively, if the white box determines that the packet is invalid or that the
30 message type of the packet is invalid it sends a negative acknowledgment to the black box side.

Referring back to figure 4, The black box determines if the white box is sending a response in the form of an incoming data word. If the black box discerns

that the white box is sending a data word the black box receives the data word and restarts the byte timer. The black box then decrypts the data word and starts to build a message packet. The black box will check this message packet and if the message packet is incomplete it will continue to receive the incoming data word from the
5   white box and will restart the byte timer after each check of the message packet. This continues until the message packet is complete. Once the message packet is complete the black box discerns whether a negative acknowledge message has been sent by the white box and if a negative acknowledge message has not been sent by the white box the black box discerns whether the packet is a valid packet and also
10   discerns whether the packet contains a valid message type. If both criteria are met the transmission of the response is complete.

Alternatively, if the message packet built by the black box is not a valid packet or if the message type within the packet is not valid, the black box will increment the retry counter and re transmit the original message to the white box. As long as
15   each incoming message packet built by the black box is not a valid packet or if the message type within the packet is not valid message the black box will increment the retry counter and re transmit the original message to the white box until the retry counter has a value which is greater than a maximum allowable value. Once the maximum allowable value of the retry has been obtained an error message will
20   be displayed on the visual display and once again a communication error process will be initiated.

Alternatively, if the incoming data word from the white box to the black is a negative acknowledge message the black box will continue to increment the retry counter and re transmit the message until the retry counter is greater than a
25   maximum allowable value. Once the retry counter reaches a value which is greater than maximum allowable value an error condition is displayed on the visual display and system 10 initiates a communication error process to discern why the negative acknowledge message is being sent.

If the response from the white box is not an incoming data word and a
30   message timer and a byte timer is less than predetermined values the black box will continue to poll for an incoming word. If the black box is receiving a response from a white box which is not an incoming data word and the message timer and the byte timer are greater than predetermined values the black box will increment the retry

counter and re transmit the message to the white box. The black box will continue
this process until the retry counter is greater than a maximum allowable value.
Once the retry counter reaches a value which is greater than maximum allowable
value an error condition is displayed on the visual display and system 10 initiates a
5   communication error process to discern the cause of the error.

In the preferred embodiment, the second processing area is the master
communication device and initiates all messages. The first processing area is the
slave and transmits data only when polled by the master. All message data shall be
encrypted to provide data security. Preferably, each incoming data word includes a
10   unique identification signature which includes at least one leading bit and at least
one trailing bit attached to the ends of the data word. By checking the leading and
trailing bits of each data word the system can discern the validity of the
identification signature of each data word. Alternatively, each completed packet can
include a unique identification signature which includes at least one leading bit and
15   at least one trailing bit attached to the ends of the message. By checking the leading
and trailing bits of each message the system can discern the validity of the
identification signature of each message.

The gaming device 100 includes an input/output device 122 for reception of a
player memory card 280 that the device 100 can read and write to. The device may
20   also include a separate stand alone station where the player can take the player
memory card for a status diagnostic including the relative ranking of the player
during the course of play or at the end of the set period for play including an
opportunity to redeem awards associated with player performance.

More particularly, and with reference to figures 1 and 2, the gaming device
25   100 is shown according to one form of the invention. The gaming device 100
includes a housing 101 that supports therewithin, a display 50 to an area for
receiving a wager 52,54 a place 122 to receive a player memory card, a display 120
that allows supplemental information to be received thereon, a plurality of decision
making buttons 102 through 116 and optionally a handle which can be used in lieu
30   of one of the decision making buttons in order to initiate play of the game. In
addition, a payout hopper 56 can be included for a redeeming awards based on play
in using the gaming device 100.

Figure 8 reflects details of the player memory card 280 and its relationship to a read/write machine interface 122 that receives the player memory card 280. More particularly, the player memory card 280 can be configured as a substantially planer rectangular piece of plastic which can include encoding on a magnetic strip 282 and includes an input/output interface 284 that can be read by the read/write machine interface 122 shown in figure 8. In essence, the input/output interface 284 is operatively coupled to an integrally formed processor or storage unit 286 contained in the player memory card 20 and the processor or storage unit 286 interfaces with an electrically erasable programmable read only memory 288 or other black box circuitry so that the ongoing status of the player's gaming activities can be uploaded and downloaded to and from the machine 100. In addition, automatic downloading of the player's descriptive information (name, address, social security number, etc.) is preferably accomplished when the memory card is in the read/write machine interface 122. This information is used for, *inter alia*, marketing use by the casino. The magnetic strip 282 can include other information if desired, such as player identification or a form of encryption for detecting the validity of the player memory card 280. In addition, the processor 286 and its memory 288 can be included with encryption or decoding means so that appropriate "handshaking" can occur between the machine interface 121 and the card 280 to minimize the likelihood of cards which have been updated by an improper unauthorized technique.

In use and operation, and referring to figure 6, the secure processing area 60 includes a processor board 162, a main board 164 and a back plane 166 integrally or separately formed. The processor board 162 includes a graphics system processor 168 which is operatively coupled to the main board 164. The main board 164 preferably includes memory in the form of ROM, RAM, flash memory and EEPROM (electrically erasable programmable read only memory). The ROM includes the EPROM 68. In addition, the main board 164 includes a system event controller, the random number generator 62, a win decoder/pay table, status indicators, a communications handler and a display/sound generator.

The main board 164 is operatively coupled to the back plane 166 which includes memory preferably in the form of an EEPROM and connectors to connect to peripherals. Furthermore, the back plane 166 provides a plurality of communication ports for communicating with external peripherals. The back plane

166 provides the coupling between discrete inputs 170 and the processor 168 and main board 164. Typical examples of elements which provide discrete inputs are coin acceptors, game buttons, mechanical hand levers, key and door switches and other auxiliary inputs. Furthermore, the back plane 166 provides the coupling

5   between discrete outputs 172 and the processor and main board 164. Typically, elements which provide discreet outputs are in the form of lamps, hard meters, hoppers, diverters and other auxiliary outputs.

The back plane 166 also provides connectors for at least one power supply 174 for supplying power for the second processing area 60 and a parallel display interface

10   "PDI" 176 and a serial interface for linking with the first processing area 20. The communication link 30 between the black box and the white box is via the parallel display interface 176 and/or the serial interface 178. In addition, the back plane 166 also provides connectors for a sound board 180 and a high resolution monitor 182. Furthermore, the back plane 166 includes communication ports for operatively

15   coupling and communicating with an accounting means 184, a touch screen 186, the bill validator 54, a printer 188, an accounting network 190, a progressive current loop 192 and an auxiliary serial link 194.

The back plane 166 optionally includes connectors for external video sources 200, expansion busses 202, slot or other display means 204, a SCSI port 208 and the

20   card reader 122 and key pad 123. The back plane 166 also preferable includes means for coupling a plurality of reel driver boards 220 which drive physical slot reels 222 with a shaft encoder or other sensor means to the processor 168 and main board 164.

Referring to figure 7, the white box can be an interactive multi-media gaming computer which includes the first processing area 20. The first processing area 20

25   includes an input/output parallel and serial card 22. The input/output card 22 is operatively coupled to a first processing area processor board 252. The processor board 252 preferably includes memory in the form of read only memory, the dynamic random access memory 26 and internal alterable program storage media 24, for example, flash memory and electrically erasable programmable read only

30   memory. In addition, the processor board 252 includes a communications handler, a display output generator and a sound output generator. The processor board 162 is operatively coupled to a video card 250 with video memory which in turn is operatively coupled to the visual display means 50.

        The processor board also allows peripherals in the form of, for example, hard
drives 254, CD ROMS 256, network interfaces 258, sound cards 260 and other
desirable peripherals 262 for game enhancement and patron entertainment.

        Moreover, having thus described the invention, it should be apparent that
numerous structural modifications and adaptations may be resorted to without
departing from the scope and fair meaning of the instant invention as set forth
hereinabove and as described hereinbelow by the claims.

CLAIMS

I Claim:

Claim 1 - A gaming machine comprising, in combination:

a first processor having a visual display and a communication interface;

a second processor sending communicating data with said first processor via said communicating interface,

said second processor having means for sensing wagering activity and means for transmitting a random gaming outcome to said first processor to be animated on said visual display,

said second processor provided with means to bestow credits as a function of the random gaming outcome.

Claim 2 - The gaming machine of claim 1 wherein said second processor includes a non-alterable memory means for storing critical gaming functions therein.

Claim 3 - The gaming machine of claim 2 wherein said second processor includes a random access memory for storing accounting and gaming outcome information therein.

Claim 4 - The gaming machine of claim 2 wherein said non-alterable memory means includes an interface to couple with an external program validation device.

Claim 5 - The gaming machine of claim 4 wherein said random access memory of second processor includes means for interfacing with an external device validation process for directly validating the outcome of any game.

Claim 6 - The gaming device of claim 1 wherein said second processor includes a random number generator for determining the random gaming output.

Claim 7 - The gaming device of claim 1 wherein said first processor includes an alterable program storage media for storing interactive multi-media gaming functions downloaded from a remote source without interfering with critical gaming programs and functions stored in the second processing area.

Claim 8 - A method for providing gaming security, the steps including:

sequestering gaming functions into two processing areas, and

linking the two processing areas via a security protocol.

Claim 9 - The method of claim 8 including forming said two processing areas into a first processing area and a second processing area,

providing the first processing area with player stimulus,

provining the second processing area with a response from the player as a function of player stimulus, and having the second processing area drive the first processing area as a result of player response.

Claim 10 - A gaming device security system operatively coupled to at least one gaming machine, the system comprising in combination:

a first processing means operatively coupled to and driving a visual display;

a second processing means operatively coupled to said first processing means and communicating therewith via a secure protocol;

a plurality of inputs enabled by a player allowing the player to initiate and sustain game play on at least the one gaming machine;

said second processing means including means for determining random outcomes of game play and means for transmitting said outcomes to said first processing means for updating said visual display;

a player memory card including memory storage means on said card removable from and accessible by to said second processing means to upload and download information between said second processing means and said player memory card reflective of status of an ongoing game.

Claim 11 - A gaming device security system, comprising in combination:

a first processor;

a second processor including a non-alterable memory means for storing critical gaming functions therein;

a communication link operatively coupled to said first processor and said second processor for transmitting encrypted data packets correlative of said critical gaming functions and outcomes.

Claim 12 - The system of claim 11 wherein said encrypted data packets include an encrypted data message and a unique identification signature to be validated upon receipt.

Claim 13 - The system of claim 12 wherein said unique identification signature includes at least one leading bit and at least one trailing bit attached to ends of said data message.

Claim 14 - The system of claim 13 further including means for checking said leading and said trailing bits of each data packet for validity of the identification signature.

Claim 15 - The system of claim 14 further including means for validating each data message of each data packet.

1/8
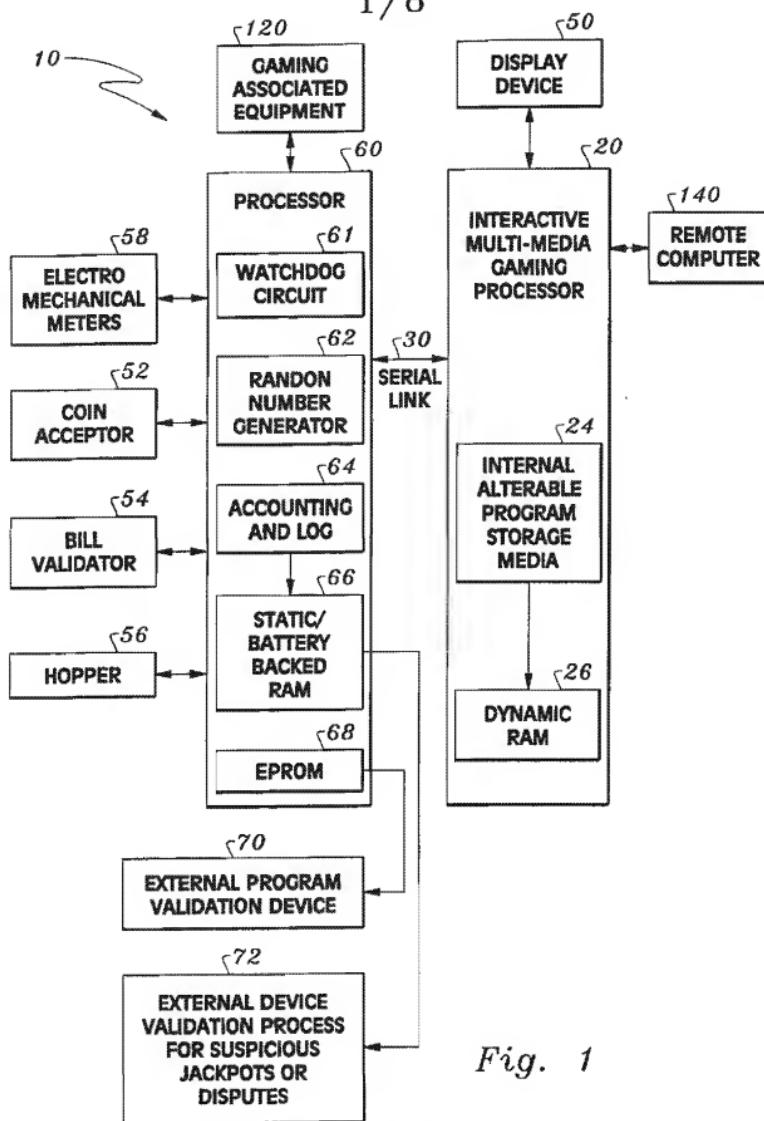
Fig. 1
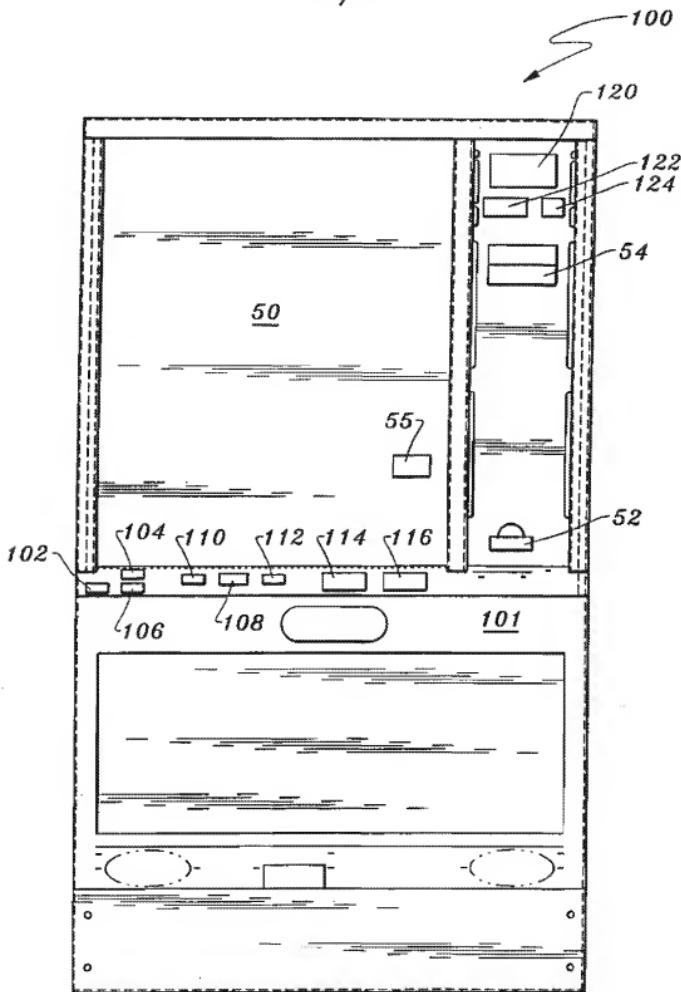
Fig. 2

3/8

BLACK BOX FLOW DIAGRAM FOR TYPICAL GAME SEQUENCE

Fig. 3

SUBSTITUTE SHEET (RULE 26)
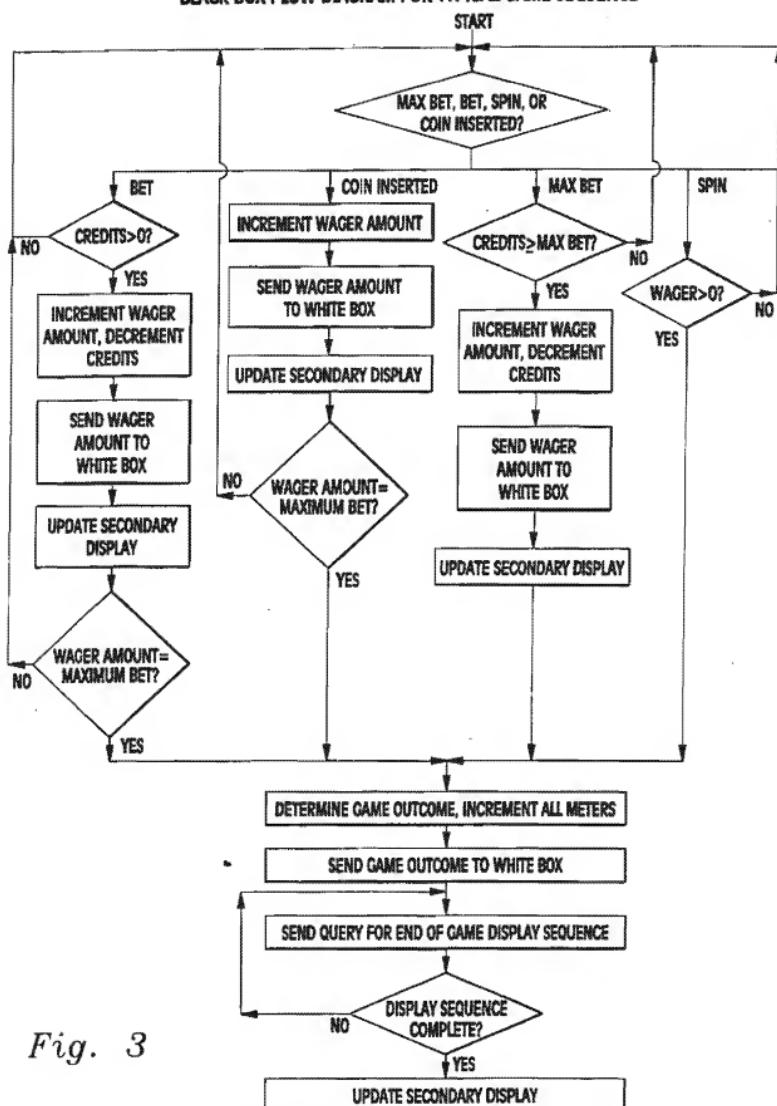
**TYPICAL POLL PROCESSING LOGIC
BLACK BOX SIDE**
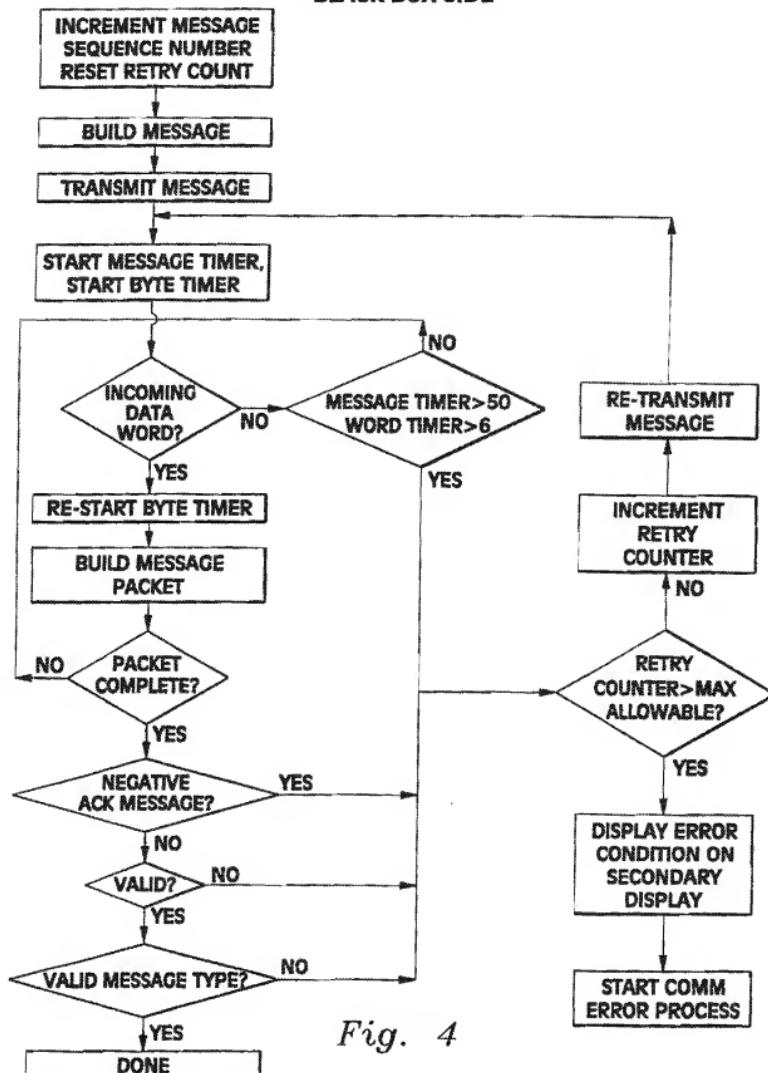
Fig. 4

5/8

TYPICAL POLL PROCESSING LOGIC
WHITE BOX SIDE
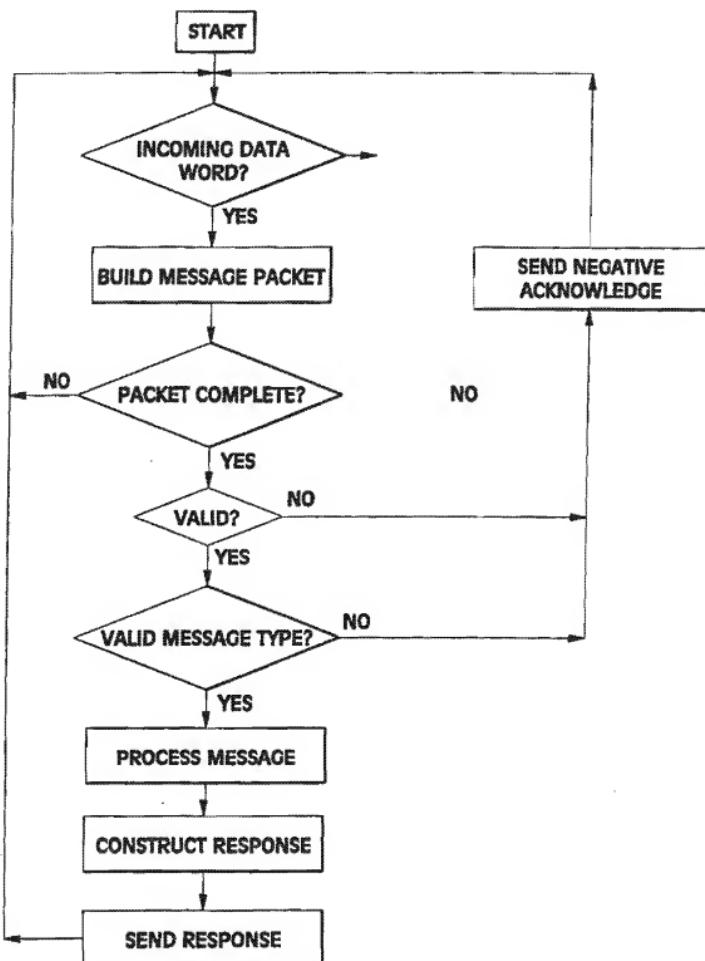
Fig. 5
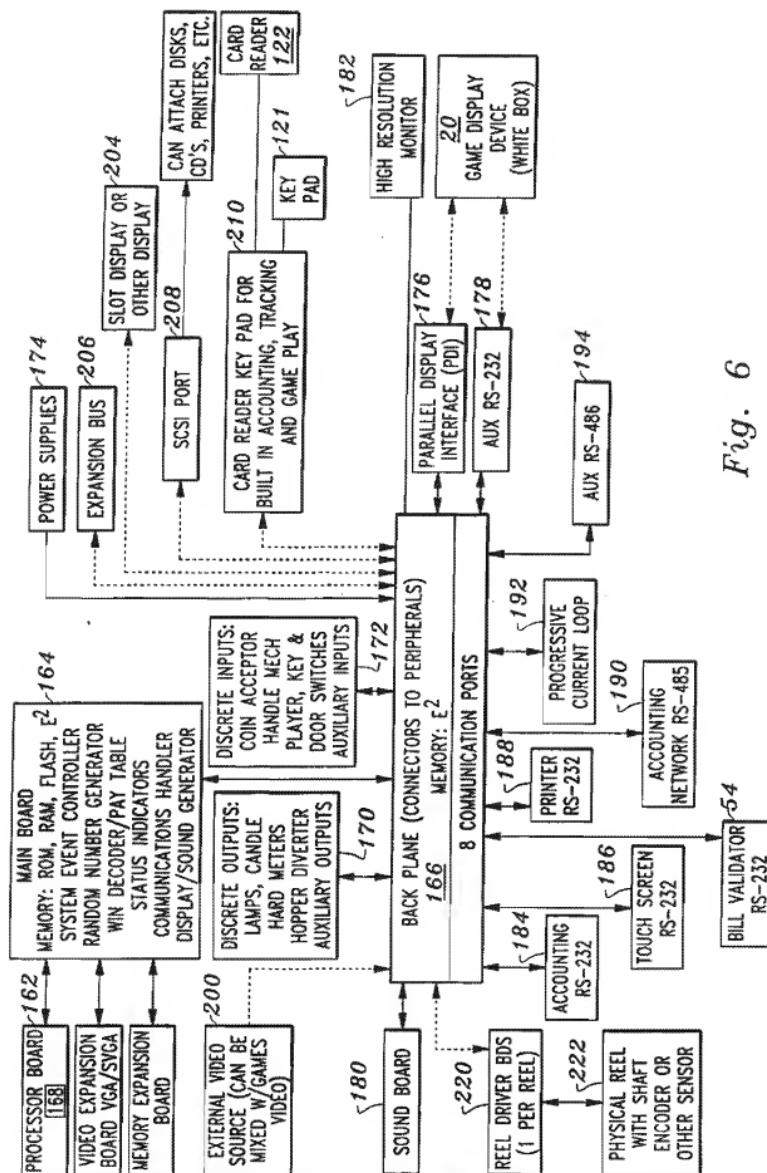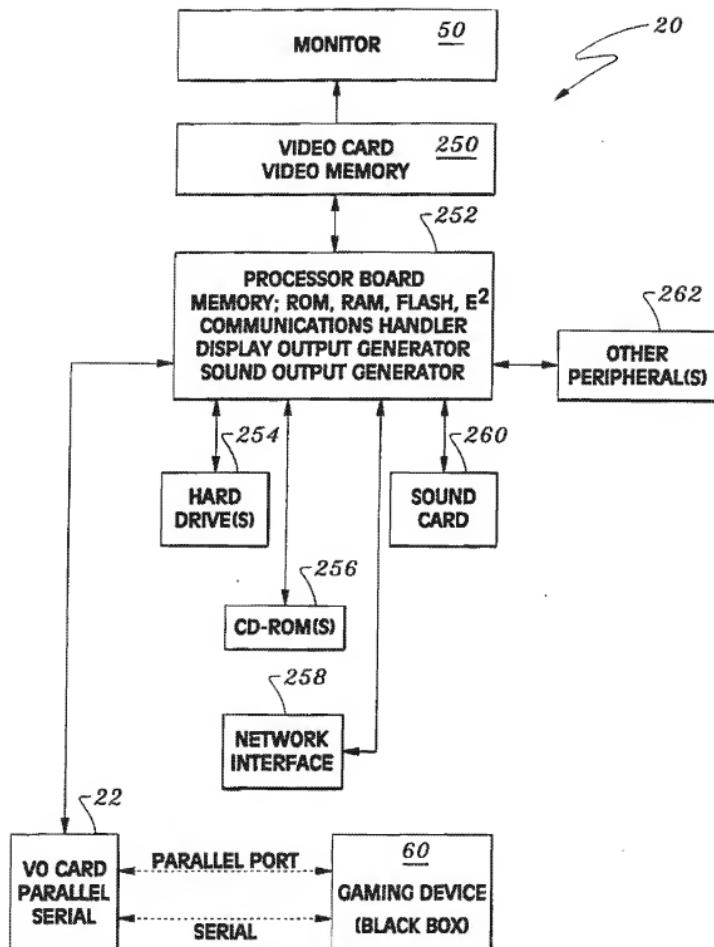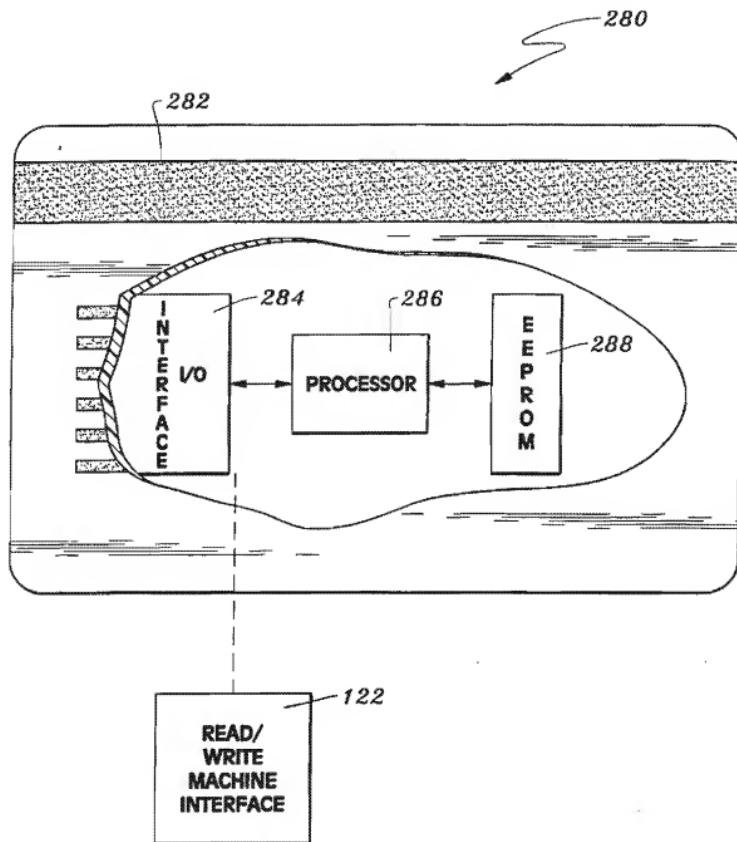
Fig. 6

7/8

*Fig. 7*

Fig. 8

A.	CLASSIFICATION OF SUBJECT MATTER

IPC(6) :A63F 9/22
US CL :380/23; 463/29, 22
According to International Patent Classification (IPC) or to both national classification and IPC

B.	FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/23; 463/29, 22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C.	DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,586,937 A (MENASHE) 24 December 1996	1-15
A, P	US 5,766,076 A (PEASE, et al.) 16 June 1998	1-15
A, P	US 5,772,509 A (WEISS) 30 June 1998	1-15
A, P	US 5,779,545 A (BERG, et al.) 14 June 1998	1-15

☐ Further documents are listed in the continuation of Box C.   ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 JULY 1998	1 5 OCT 1998

Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	DAVID CAIN
Facsimile No. (703) 305-3230	Telephone No. (703) 305-1836